

**IN THE UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF NEW YORK**

CAROL KANE, *on behalf of herself and
all others similarly situated,*

Plaintiff,

v.

UNIVERSITY OF ROCHESTER
MEDICAL CENTER,

Defendant.

Case No. 23-cv-6027

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

CLASS ACTION COMPLAINT

Plaintiff Carol Kane (“Plaintiff”) brings this class action lawsuit in her individual capacity and on behalf of all others similarly situated against University of Rochester Medical Center (“URMC” or “Defendant”) and alleges, upon personal knowledge as to her own actions and experiences, her counsel’s investigation and upon information and good faith belief as to all other matters, as follows:

1. As detailed herein, this case arises from Defendant’s intentional, reckless, and negligent disclosure of Plaintiff’s and Class Members’ confidential and private medical information to Meta Platforms, Inc., d/b/a Meta (“Facebook”), both of which benefitted from Defendant’s marketing program at the expense of its patients’ privacy.

2. URMC failed to properly secure and to safeguard personally identifiable information (“PII”) and non-public personal health information (“PHI”)¹ including, but not limited to, individual patients’ computer IP addresses, physical locations, appointment information,

¹ This information is collectively referred to as “PII and PHI” or collectively, “Private Information.”

medical provider information, unique and persistent Facebook IDs, and other confidential information submitted on Defendant's website and patient portal.²

3. Defendant encouraged Plaintiff and Class Members to use its digital tools via its website, <https://www.urmc.rochester.edu/> (the "Website") in order to receive healthcare services, and Plaintiff and Class Members did so with the reasonable and appropriate understanding that Defendant would secure and maintain any PII and PHI provided as confidential.

4. At all times that they visited and utilized Defendant's Website, Plaintiff and Class Members had a reasonable expectation of privacy that any Private Information collected through Defendant's Website would remain secure and protected and only accessible by UPMC to be utilized for medical purposes.

5. Plaintiff and Class Members provided Private Information to Defendant in order to receive medical services rendered and with the reasonable expectation that Defendant would protect their Private Information.

6. Plaintiff and Class Members relied on Defendant to secure and to protect the Private Information and not disclose same to unauthorized third parties without their knowledge or informed consent.

7. Defendant further made express and implied promises to protect Plaintiff's and Class Members' Private Information and to maintain the privacy and confidentiality of communications that patients exchanged with Defendant.

² Defendant's website is available at <https://www.urmc.rochester.edu/> (last visited December 23, 2022).

8. Defendant owed common law, contractual, statutory, and regulatory duties to keep Plaintiff's and Class Members' communications and medical information safe, secure, and confidential.

9. Furthermore, by obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' Private Information, Defendant assumed legal and equitable duties to those individuals to protect and to safeguard that information from unauthorized disclosure.

10. Defendant, however, failed in its obligations and promises by utilizing the Facebook Pixel, described below, on its Website knowing that such technology would transmit and share Plaintiff's and Class Members' Private Information with unauthorized third parties.

11. Defendant's Website encourages patients to exchange communications to search for a doctor, learn more about their conditions and treatments, make appointments, and access medical records and test results.

12. Defendant intentionally installed the well-known Facebook tracking pixel (the "Pixel") on its Website that secretly enabled the unauthorized transmission and disclosure of Plaintiff's and Class Members' confidential medical information.

13. A pixel is a piece of code that "tracks the people and type of actions they take."³

14. Pixels are routinely used to target specific customers by utilizing the data gathered through the pixel to build profiles for the purposes of retargeting and future marketing.

15. Upon information and belief, Defendant utilized the Pixel data to improve and to save costs on its marketing campaigns, improve its data analytics in order to increase revenues by, among other things, attracting new patients and providing more services to existing patients.

³ FACEBOOK, RETARGETING, <https://www.facebook.com/business/goals/retargeting> (last visited Dec. 23, 2022).

16. Operating as designed, Defendant's tracking Pixel allowed the Private Information that Plaintiff and Class Members submitted to Defendant to be unlawfully disclosed to Facebook.

17. For example, when Plaintiff or a Class Member accessed Defendant's Website hosting the tracking Pixel, the Facebook software directed Plaintiff's or Class Members' browser to send a message to Facebook's servers.

18. The information sent to Facebook by Defendant included the Private Information that Plaintiff and Class Members submitted to Defendant's Website including, but not limited to, the type of medical treatment an individual is seeking; the name, gender, and specialty of physicians with whom individuals schedule appointments; and the locations where individuals seek treatment.

19. Such Private Information would allow a third party (e.g., Facebook) to know that a specific patient was seeking confidential medical care. This type of disclosure could also allow a third party to reasonably infer that a specific patient was being treated for a specific type of medical condition such as cancer, pregnancy or AIDS.

20. The exposed Private Information of Plaintiff and Class Members can—and likely will—be further disseminated to additional third parties utilizing the data for retargeting or insurance companies utilizing the information to set insurance rates.

21. Furthermore, third parties can often offer for sale the unencrypted, unredacted Private Information to criminals on the dark web for use in fraud and cyber-crimes.

22. Defendant has not disclosed to Plaintiff or Class Members that it shares patients' sensitive and confidential communications via the Website with Facebook.

23. As a result, Plaintiff and Class Members were unaware that their PII and PHI were being surreptitiously transmitted to Facebook as they communicated with their healthcare provider.

24. Defendant breached its obligations in one or more of the following ways: (i) failing to adequately review its marketing programs and web based technology to ensure the Website was safe and secure; (ii) failing to remove or disengage technology that was known and designed to share web users' information; (iii) failing to obtain the consent of Plaintiff and Class Members to disclose their PII and PHI to Facebook or others; (iv) failing to take steps to block the transmission of Plaintiff's and Class Members' PII and PHI through the Facebook Pixel; (v) failing to warn Plaintiff and Class Members; and (vi) otherwise failing to design, and monitor its Website to maintain the confidentiality and integrity of patient PII and PHI.

25. Plaintiff and Class Members have suffered injury as a result of Defendant's conduct; these injuries include: (i) invasion of privacy; (ii) loss of benefit of the bargain, (iii) compromise and disclosure of Private Information and identities, (iv) diminution of value of the Private Information, (iv) statutory damages, and (v) the continued and ongoing risk to their Private Information.

26. Plaintiff seeks to remedy these harms and bring causes of action for (i) Invasion of Privacy, (ii) Breach of Contract; (iii) Breach of Fiduciary Duty; (iv) Unjust Enrichment; (v) Breach of Implied Contract; (vi) Violation of New York's Deceptive Trade Practices Act (New York Gen. Bus. Law § 349); (vii)-(viii) Violation of the Wiretap Act (18 U.S.C. § 2510 *et seq.*); (ix) Violation of the Stored Communications Act (18 U.S.C. § 2702 *et seq.*); and (x) Violation of the Computer Fraud and Abuse Act (18 U.S.C. § 1030 *et seq.*).

PARTIES

27. Defendant UPMC is a registered non-profit entity with its headquarters and principal place of business at 601 Elmwood Ave, Rochester, New York.

28. Defendant UPMC is one of the largest facilities for medical treatment and research in upstate New York, employing more than 26,000 employees and nearly 3,000 clinical researchers.

29. Defendant is a covered entity under the Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. § 1320d and 45 C.F.R. Part 160-45 C.F.R. Part 162, and 45 C.F.R. Part 164 (“HIPAA”).

30. Plaintiff Carol Kane is a natural person and citizen of Florida.

31. Plaintiff Kane accessed Defendant’s Website on her mobile device and computer as recently as November 2022 and used the Website to look for providers.

32. Plaintiff has used and continues to use the same devices to maintain and to access an active Facebook account throughout the relevant period in this case.

33. Further to the systematic process described herein, UPMC assisted Facebook with intercepting Plaintiff’s communications, including those that contained personally identifiable information, protected health information, and related confidential information.

34. Defendant assisted these interceptions without Plaintiff Kane’s knowledge, consent, or express written authorization. By failing to receive the requisite consent, Defendant breached confidentiality and unlawfully disclosed Plaintiff Kane’s personally identifiable information and protected health information.

JURISDICTION & VENUE

35. This Court has subject matter jurisdiction over this action under 28 U.S.C. § 1331

because it arises under the laws of the United States, and under 28 U.S.C. § 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of \$5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the class is a citizen of a state different from Defendant..

36. This Court has personal jurisdiction over Defendant because its principal place of business is in this District and a substantial portion of the acts and omissions giving rise to Plaintiffs' claims occurred in and emanated from this District.

37. Venue is proper under 18 U.S.C § 1391(b)(1) because Defendant's principal place of business is in this District.

COMMON FACTUAL ALLEGATIONS

Defendant Improperly Disclosed Plaintiff's & Class Members' Private Information

38. Defendant UPMC's clinical enterprise, UR Medicine, consists of six hospitals located throughout the Finger Lakes and Southern Tier regions – Strong Memorial, Highland, F.F. Thompson, Noyes Memorial, Jones Memorial, and St. James hospitals, as well as Golisano Children's Hospital, James P. Wilmot Cancer Center, Eastman Institute for Oral Health, University of Rochester Medicine Home Care, the Highlands at Pittsford retirement community and Highlands at Brighton nursing home, nine urgent care centers, and an extensive primary care network.

39. As the owner and operator of these medical centers and entities, Defendant UPMC offers a wide range of services, from primary and urgent care to cancer treatment, cardiac and liver transplants, heart and vascular, orthopedics, hospice care, occupational health and senior living.

40. Defendant's Website, <https://www.upmc.rochester.edu/>, is accessible on mobile devices and desktop computers.

41. Defendant utilized Facebook advertisements and intentionally installed the Pixel on its Website.

42. The Pixel is a piece of code that Defendant commonly used to measure activity and experiences on its Website.

43. Through seeking and using Defendant's services as a medical provider, and utilizing the Website services, Plaintiff's and Class Members' Private Information was intercepted in real time and then disseminated to Facebook, and potentially to other third parties, via the Pixel that Defendant surreptitiously installed on its Website.

44. Plaintiff and Class Members did not intend or have any reason to suspect the Private Information would be shared with Facebook or that Defendant was tracking their every movement and disclosing same to Facebook when they provided highly sensitive information on the Website.

45. Defendant did not disclose to or warn Plaintiff or Class Members that Defendant used the Private Information contained in Plaintiff's and Class Members' Website submissions for marketing purposes.

46. Plaintiff and Class Members never consented, agreed, authorized, or otherwise permitted Defendant to disclose their Private Information.

47. Upon information and belief, Defendant intercepted and disclosed the following non-public private information to Facebook:

- a. Plaintiff's and Class Members' status as medical patients;
- b. Plaintiff's and Class Members' communications with Defendant through its Website;
- c. Plaintiff's and Class Members' medical appointments, location of treatments, specific medical providers, and specific medical

conditions and treatments;

- d. Personally identifiable information including but not limited to patients' locations, an IP address, device identifier, and/or an individual's unique Facebook user number ("FID").

48. Defendant deprived Plaintiff and Class Members of their privacy rights when they: (i) implemented technology (*i.e.*, Pixels) that surreptitiously tracked, recorded, and disclosed Plaintiff's and other online patients' confidential communications and Private Information; (ii) disclosed patients' protected information to Facebook—an unauthorized third-party; and (iii) undertook this pattern of conduct without notifying Plaintiff or Class Members and without obtaining their express written consent.

Operation Source Code

49. Web browsers are software applications that allow consumers to exchange electronic communications over the Internet.

50. Every website is hosted by a computer server through which the entity in charge of the website exchanges communications with Internet users via their web browsers.

51. The set of instructions that commands the browser is called the source code.

52. Source code may also command a web browser to send data transmissions to third parties via pixels or web bugs, tiny 1x1 invisible GIF files that effectively open a spying window through which a website funnels data about users and their actions to third parties.

53. The third parties to whom the website transmits data through pixels or web bugs do not provide any substantive content relating to the user's communications. Instead, these third parties are typically configured to track user data and communications for marketing purposes.

54. The web bugs are tiny and camouflaged to purposefully remain invisible to the user.

55. Thus, without any knowledge, authorization, or action by a user, a website developer like Defendant URM C can use its source code to commandeer the user's computing device, causing the device to contemporaneously and invisibly re-direct the users' personally identifiable non-public medial information to third parties.

The Facebook Pixel

56. Defendant secretly deployed the Pixel on their Website in violation of its common law, contractual, statutory, and regulatory duties and obligations.

57. The Facebook Pixel, a marketing product, is a "piece of code" that allowed Defendant to "understand the effectiveness of [their] advertising and the actions [patients] take on [their] site."⁴

58. The Pixel also permitted Defendant to optimize the delivery of ads, measure cross-device conversions, create custom audiences, learn about the Website, and decrease advertising and marketing costs.⁵

59. Most importantly, it allowed Defendant and Facebook to secretly track patients on Defendant's Website and intercept their communications with same.

Facebook's Platform and its Business Tools

60. Facebook operates the world's largest social media company.

61. In 2021, Facebook generated \$117 billion in revenue.⁶ Roughly 97% of that came

⁴ <https://www.facebook.com/business/help/742478679120153?id=1205376682832142> (last visited Dec. 23, 2022).

⁵ *Id.*

⁶ FACEBOOK, META REPORTS FOURTH QUARTER AND FULL YEAR 2021 RESULTS, <https://investor.fb.com/investor-news/press-release-details/2022/Meta-Reports-Fourth-Quarter-and-Full-Year-2021-Results/default.aspx> (last visited Dec. 23, 2022).

from selling advertising space.⁷

62. As a core part of its business, Facebook maintains profiles on users that include the user’s real names, locations, email addresses, friends, likes, and communications that Facebook associates with personal identifiers, including IP addresses.

63. Facebook also tracks non-Facebook users through its widespread internet marketing products and source code.

64. Facebook then sells advertising space by highlighting its ability to target users.⁸

65. Facebook can target users so effectively because it surveils user activity both on and off its site.⁹

66. This allows Facebook to make inferences about users beyond what they explicitly disclose, like their “interests,” “behavior,” and “connections.”¹⁰

67. Facebook compiles this information into a generalized dataset called “Core Audiences,” which advertisers use to apply highly specific filters and parameters for their targeted advertisements.¹¹

68. Indeed, Facebook utilizes the precise type of information disclosed by Defendant

⁷ *Id.*

⁸ FACEBOOK, WHY ADVERTISE ON FACEBOOK, <https://www.facebook.com/business/help/205029060038706> (last visited Dec. 23, 2022).

⁹ FACEBOOK, ABOUT FACEBOOK PIXEL, <https://www.facebook.com/business/help/742478679120153?id=1205376682832142> (last visited Dec. 23, 2022).

¹⁰ FACEBOOK, AD TARGETING: HELP YOUR ADS FIND THE PEOPLE WHO WILL LOVE YOUR BUSINESS, <https://www.facebook.com/business/ads/ad-targeting> (last visited Dec. 23, 2022).

¹¹ FACEBOOK, EASIER, MORE EFFECTIVE WAYS TO REACH THE RIGHT PEOPLE ON FACEBOOK, <https://www.facebook.com/business/news/Core-Audiences> (last visited Dec. 23, 2022).

to identify, target, and market products and services to individuals.

69. Advertisers can also build “Custom Audiences.”¹² Custom Audiences enable advertisers to reach “people who have already shown interest in [their] business, whether they’re loyal customers or people who have used [their] app or visited [their] website.”¹³ With Custom Audiences, advertisers can target existing customers directly, and they can also build a “Lookalike Audiences,” which “leverages information such as demographics, interests, and behavior from your source audience to find new people who share similar qualities.”¹⁴

70. Unlike Core Audiences, advertisers can build Custom Audiences and Lookalike Audiences only if they first supply Facebook with the underlying data. They can do so through two mechanisms: by manually uploading contact information for customers, or by utilizing Facebook’s “Business Tools.”¹⁵

71. As Facebook puts it, the Business Tools “help website owners and publishers, app developers and business partners, including advertisers and others, integrate with Facebook, understand and measure their products and services, and better reach and serve people who might

¹² FACEBOOK, ABOUT CUSTOM AUDIENCES, <https://www.facebook.com/business/help/744354708981227?id=2469097953376494> (last visited Dec. 23, 2022).

¹³ FACEBOOK, AD TARGETING, HELP YOUR ADS FIND THE PEOPLE WHO WILL LOVE YOUR BUSINESS, <https://www.facebook.com/business/ads/ad-targeting> (last visited Dec. 23, 2022).

¹⁴ FACEBOOK, ABOUT LOOKALIKE AUDIENCES, <https://www.facebook.com/business/help/164749007013531?id=401668390442328> (last visited Dec. 23, 2022).

¹⁵ FACEBOOK, CREATE A CUSTOMER LIST CUSTOM AUDIENCE, <https://www.facebook.com/business/help/170456843145568?id=2469097953376494>; Facebook, Create a Website Custom Audience <https://www.facebook.com/business/help/1474662202748341?id=2469097953376494> (last visited Dec. 23, 2022).

be interested in their products and services.”¹⁶

72. Put more succinctly, Facebook’s Business Tools are bits of code that advertisers can integrate into their website, mobile applications and servers, thereby enabling Facebook to intercept and collect user activity on those platforms.

73. The Business Tools are automatically configured to capture certain data, like when a user visits a webpage, that webpage’s Universal Resource Locator (“URL”) and metadata, or when a user downloads a mobile application or makes a purchase.¹⁷

74. Facebook’s Business Tools can also track other events. Facebook offers a menu of “standard events” from which advertisers can choose, including what content a visitor views or purchases.¹⁸ Advertisers can even create their own tracking parameters by building a “custom event.”¹⁹

75. One such Business Tool is the Facebook Pixel. Facebook offers this piece of code to advertisers, like Defendant, to integrate into their websites. As the name implies, the Facebook

¹⁶ FACEBOOK, THE FACEBOOK BUSINESS TOOLS, <https://www.facebook.com/help/331509497253087> (last visited Dec. 23, 2022).

¹⁷ See FACEBOOK, FACEBOOK PIXEL, ACCURATE EVENT TRACKING, ADVANCED, <https://developers.facebook.com/docs/facebook-pixel/advanced/>; see also FACEBOOK, BEST PRACTICES FOR FACEBOOK PIXEL SETUP, <https://www.facebook.com/business/help/218844828315224?id=1205376682832142>; FACEBOOK, APP EVENTS API, <https://developers.facebook.com/docs/marketing-api/app-event-api/> (last visited Dec. 23, 2022).

¹⁸ FACEBOOK, SPECIFICATIONS FOR FACEBOOK PIXEL STANDARD EVENTS, <https://www.facebook.com/business/help/402791146561655?id=1205376682832142> (last visited Dec. 23, 2022).

¹⁹ FACEBOOK, ABOUT STANDARD AND CUSTOM WEBSITE EVENTS, <https://www.facebook.com/business/help/964258670337005?id=1205376682832142>; see also FACEBOOK, APP EVENTS API, <https://developers.facebook.com/docs/marketing-api/app-event-api/> (last visited Dec. 23, 2022).

Pixel “tracks the people and type of actions they take.”²⁰

76. When a user accesses a website hosting the Facebook Pixel, Facebook’s software script surreptitiously directs the user’s browser to send a separate message to Facebook’s servers. This second, secret transmission contains the original GET request sent to the host website, along with additional data that the Facebook Pixel is configured to collect.

77. This transmission is initiated by Facebook code and concurrent with the communications with the host website. Two sets of code are thus automatically run as part of the browser’s attempt to load and read Defendant’s Website—Defendant’s own code, and Facebook’s embedded code.

78. An example illustrates the point. Take an individual who navigates to Defendant’s Website and clicks on a tab for “AIDS Center.” When that tab is clicked, the individual’s browser sends a GET request to Defendant’s server requesting that server to load the particular webpage. Because UPMC utilizes the Facebook Pixel, Facebook’s embedded code, written in JavaScript, sends secret instructions back to the individual’s browser, without alerting the individual that this is happening.

79. Facebook causes the browser to secretly duplicate the communication with UPMC, transmitting it to Facebook’s servers, alongside additional information that transcribes the communication’s content and the individual’s identity. Consequently, when Plaintiff and Class Members visited Defendant’s Website and entered, e.g., Diabetes or Bone Cancer on Defendant’s Website, their Private Information was transmitted to Facebook, including, but not limited to, physician and appointment selected, treatments and care options, and specific button/menu

²⁰ FACEBOOK, RETARGETING, <https://www.facebook.com/business/goals/retargeting>.

selections.

80. During the same transmissions, the Website would also provide Facebook with the patient's Facebook ID, IP address and/or device ID or other personally identifiable information they input into UPMC's Website.

81. This is precisely the type of information that HIPAA requires healthcare providers to de-anonymize to protect the privacy of patients.²¹

82. Plaintiff's and Class Members' identities could be easily determined based on the Facebook ID, IP address and/or reverse lookup from the collection of other identifying information that was improperly disclosed.

83. After intercepting and collecting this information, Facebook processes it, analyzes it, and assimilates it into datasets like Core Audiences and Custom Audiences. If the Website visitor is also a Facebook user, Facebook will associate the information that it collects from the visitor with a Facebook ID that identifies their name and Facebook profile, i.e., their real-world identity.

84. A user's Facebook Profile ID is linked to their Facebook profile, which generally contains a wide range of demographic and other information about the user, including pictures, personal interests, work history, relationship status, and other details. Because the user's Facebook Profile ID uniquely identifies an individual's Facebook account, Meta—or any other person—can use the Facebook Profile ID to quickly and easily locate, access, and view the user's corresponding Facebook profile.

²¹ <https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html> (last visited Dec. 23, 2022).

85. In other words, the Pixel allows Meta to know what medical content one of its users viewed on Defendant's Website.

How URMC Discloses Class Members' Protected Health Information and Assists with Intercepting Communications

86. Through the Facebook Pixel, Defendant shares its patients' identities and online activity, including information and search results related to their private medical treatment.

87. For example, when a patient visits <https://www.urmc.rochester.edu/> to search for a doctor, they may select the "Find a Provider" tab, which takes them to the "Find a Provider" page.

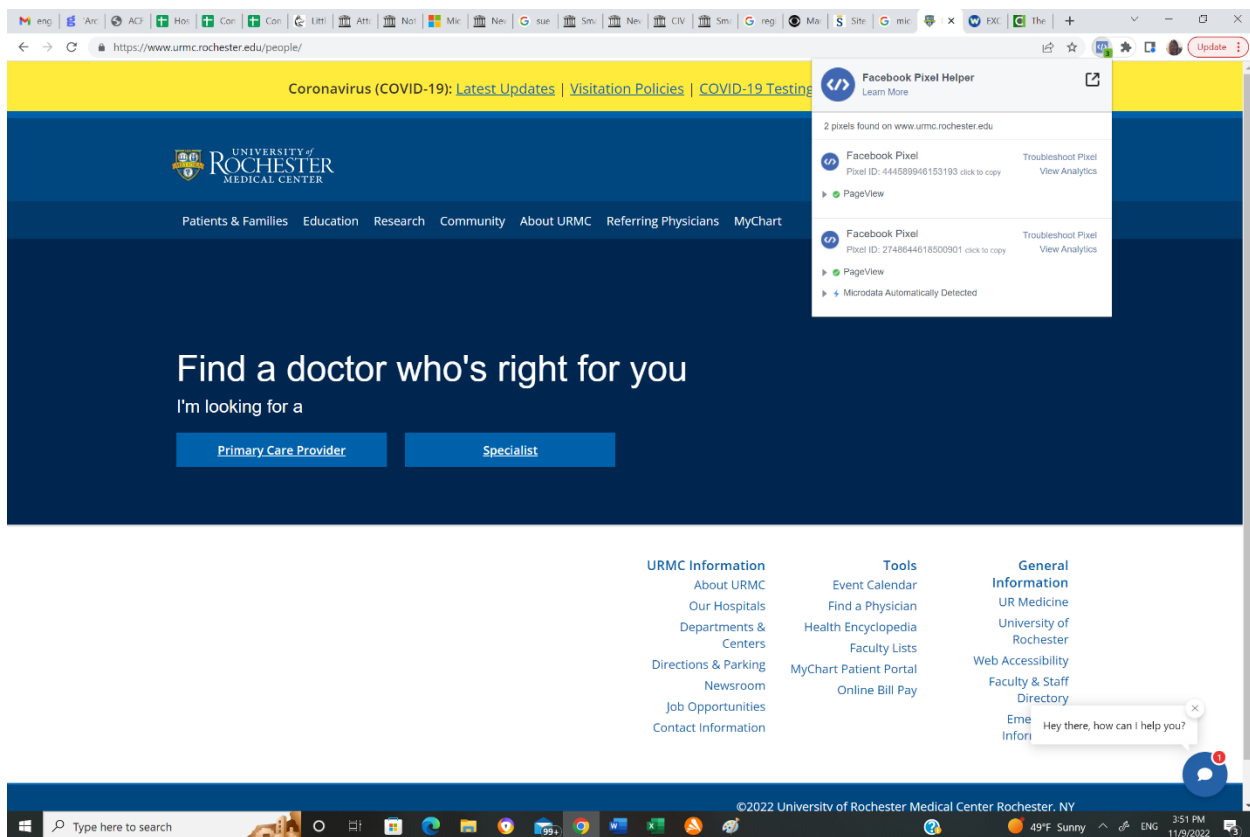


Figure 1. Defendant directs patients to its "Find a Provider" webpage with embedded Pixels.

88. If a patient selects filters or enters keywords into the search bar on the "Find a Provider" webpage, the filters and search terms are transmitted via the Facebook Pixel. Similarly, if a patient uses the Website's general search bar or chat, the terms and phrases the patient types

are transmitted to Facebook, even if they contain a patient's treatment, procedures, medical conditions, and related queries. This information is automatically sent from the patient's device to Facebook, and it reveals the patient's FID (c_user field) along with each search filter the patient selected.

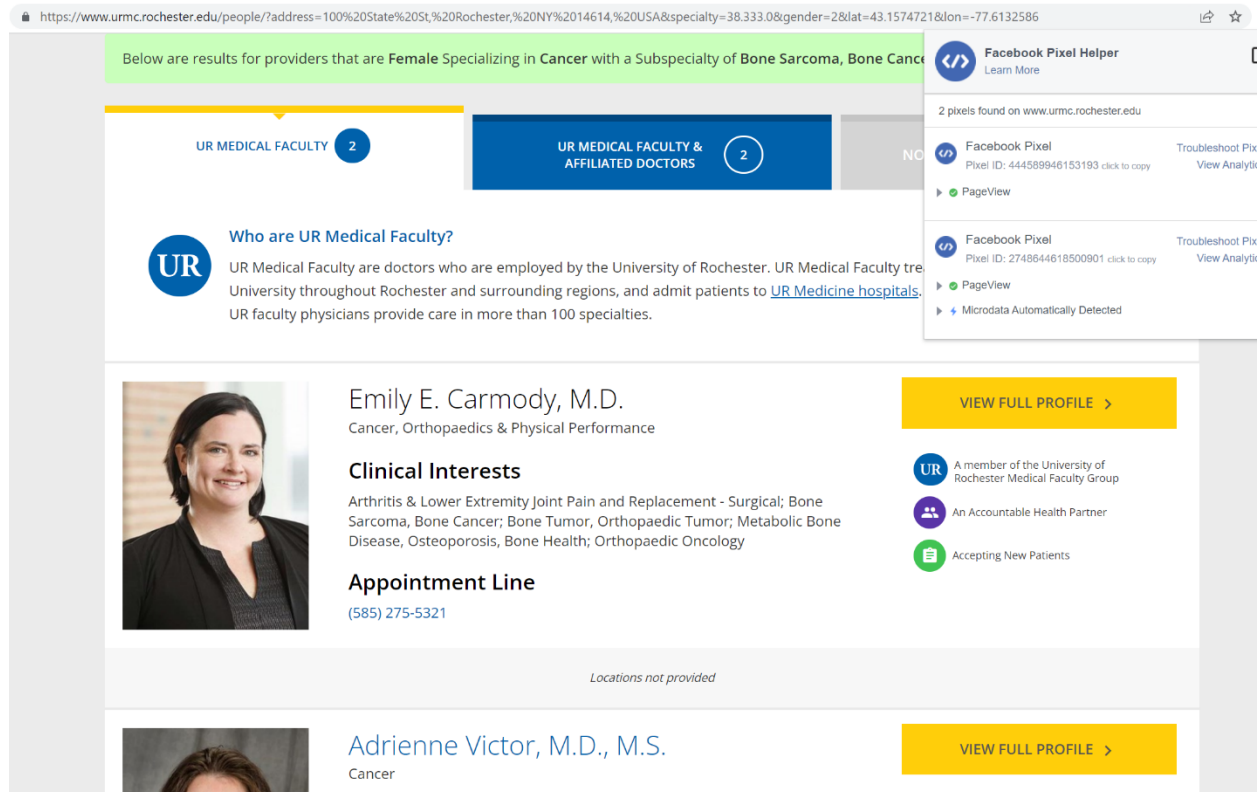


Figure 2. Example of search results for a provider specializing in “Bone Cancer” near 100 State Street, Rochester, NY, 14614.

89. After taking any of these actions on the Find a Provider page, patients are subsequently directed to the “Provider Search Results” page, and their selections or search parameters are automatically transmitted to Facebook.

```

Request Headers
:authority: www.facebook.com

:method: GET

:path: /tr/?id=2748644618500901&e=Microdata&dl=https%3A2F2Fwww.urmc.rochester.edu%2Fpeople%2F%3A%2Fspecialty%3D38.333.35%26gender%3D2&rl=if=false&ts=1671995366530&cd%5B0dataLayer%5D=%5B%5D&cd%5Bmeta%5D=%7B%22title%22%3A%22Find%20a%20Provider%20-%20University%20of%20Rochester%20Medical%20Center%22%7D&cd%5BopenGraph%5D=%7B%7D&cd%5Bschema.org%5D=%5B%5D&cd%5BJSON-LD%5D=%5B%5D&sw=1664&sh=1110&v=2.9.0&r=stable&ec=1&o=30&fbp=fb.1.1671085782832.217921790&it=1671995364843&coo=false&es=automatic&tm=3&rqm=GET&dt=c66212hbo4hna8wprc29tkoajj0l649n

:scheme: https

accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8

accept-encoding: gzip, deflate, br

accept-language: en-US,en;q=0.9,ru;q=0.8

cookie: c_user=54; datr=QtI1Y1Vd2Uw00uBmn2Mb8vc; m_page_voice=540643061; dpr=1.5; xs=188%3Awgt7jCKaF4RNPg%3A2%3A1597289338%3A-1%3A3037%3A%3AACV014XdpQIDRQwzkoey6qo_jgueDtItKEW2lPeMFA; fr=0YSVguIz0w29ucSr.AWvRkGakfu8_s0MT7iE4YedZ9o.Bjn2Qp.-f.AAA.0.0.Bjn2Qp.AWV_lzutmSE

referer: https://www.urmc.rochester.edu/

```

Figure 3. Example of data from a search result for a “Bone Cancer” provider being shared with Facebook along with the patient’s Facebook ID (c user field).

90. Once a patient chooses a doctor, all of the information that patient has submitted is automatically sent directly to Facebook. The information transmitted to Facebook includes: (i) the patient's unique and persistent Facebook ID (c_user ID), (ii) the fact that the patient clicked on a specific provider's profile page (Dr. Emily Carmody in the example above and below), (iii) the patient's search parameters (demonstrating they specifically searched for a female or male doctor and their specialty), and (iv) the patient's location.

```
> Request Headers
:authority: www.facebook.com

:method: GET

:path: /tr/?id=2748644618509091&_r=Microdata%dl=https%3A%2F%2Fwww.urmc.rochester.edu%2Fpeople%2F21760532_emily-e-carmody%l=https%3A%2F%2Fwww.urmc.rochester.edu%2Fpeople%2F%Address%100%52State%25%5t%2C%53Rochester%2C%2520NY%252146142C%2520USA%2specialty%3D38.333.0%gender%3D2%26lat%3D43.1574721%26lon%3D-77.6132586&if=false&ts=1671914465349&cd%5BdataLayer%5D=%5B%5D&cd%5Bmeta%5D=%7B%22title%22%3A%22%5cn%5ctemil%20E.%20Carmody%2C%20M.D.%20-%20%20University%20of%20Rochester%20Medical%20Center%5Cn%22%7D&cd%5BopenGraph%5D=%7B%7D&cd%5Bschema.org%5D=%5B%5D&cd%5BJSON-LD%5D=%5B%5D&sw=1664&sh=1110&v=2.9.0&r=stable&ec=1&o=30&fbp=fb-1.1671085782832.217921790&it=1671914463591&coo=false&es=automatic&tcm=3&rqm=GET&dt=qw85booaajg%5eqpiczajpsjh5jp4aftw

:scheme: https

accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8

accept-encoding: gzip, deflate, br

accept-language: en-US,en;q=0.9,ru;q=0.8

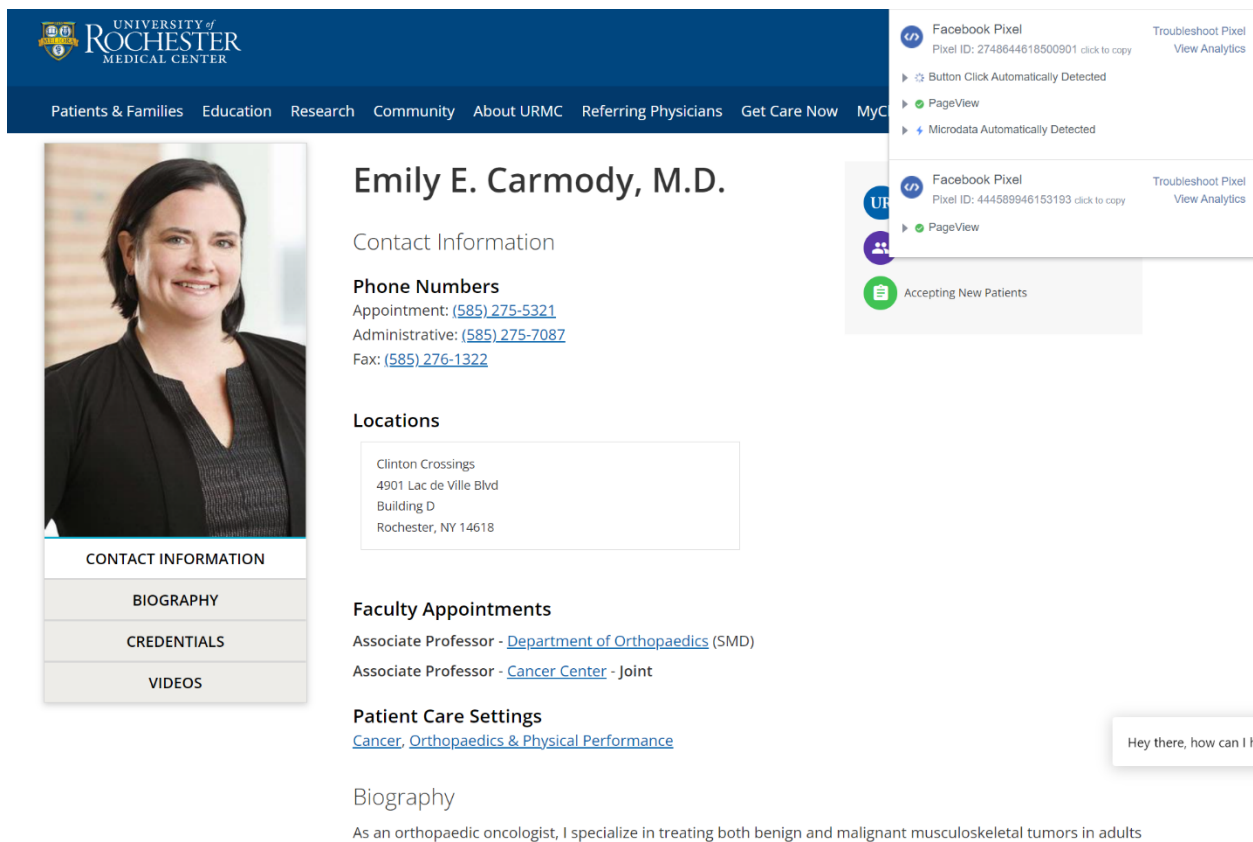
cookie: c_user=54.; datr=QIT1IY1Vd2UWou8mn2Mb8vc; m_page_voice=540643061; dpr=1.5; xs=188%3AwGtj7jCKaFARNpg%3A2%3A1597289338%3A-1%3A3037%3A%3AACVC14XdppQIDQRQwkoeY6qo_jgueDTITEK2N1PeMfa; fr=0YSvguiZoZw29ucsr.AwVrkGakfu8_s0MTie74YEYZ90.Bjn2Qp.-f.AAA.0.0.Bjn2Qp.AwV_lztutMSE

referer: https://www.urmc.rochester.edu/
```

Figure 4. Defendant’s transmission to Facebook of patient’s search parameters showing search terms including patient’s address (the US District Court in this instance), search results displayed to patient, and the patient’s FID (c user field) information.

91. Defendant's website also includes a feature that allows patients to book appointments through a particular doctor's profile page. If a patient clicks on the "Schedule an

Appointment” button, this action is communicated and shared with Facebook. Facebook classifies this event as a “SubscribedButtonClick,” which indicates that the patient clicked the specific button (in order to book the appointment). Similarly, each doctor’s profile page includes a direct link that allows a patient to call the doctor’s office, and, upon clicking the telephone number button, the patient’s click is shared with Facebook.



UNIVERSITY of ROCHESTER MEDICAL CENTER

Patients & Families Education Research Community About URMC Referring Physicians Get Care Now MyC

Emily E. Carmody, M.D.

Contact Information

Phone Numbers
 Appointment: [\(585\) 275-5321](tel:(585)275-5321)
 Administrative: [\(585\) 275-7087](tel:(585)275-7087)
 Fax: [\(585\) 276-1322](tel:(585)276-1322)

Locations

Clinton Crossings
 4901 Lac de Ville Blvd
 Building D
 Rochester, NY 14618

CONTACT INFORMATION

BIOGRAPHY

CREDENTIALS

VIDEOS

Faculty Appointments
 Associate Professor - [Department of Orthopaedics](#) (SMD)
 Associate Professor - [Cancer Center](#) - Joint

Patient Care Settings
[Cancer, Orthopaedics & Physical Performance](#)

Biography

As an orthopaedic oncologist, I specialize in treating both benign and malignant musculoskeletal tumors in adults

Facebook Pixel
 Pixel ID: 2748644618500901 click to copy
 Troubleshoot Pixel View Analytics

Button Click Automatically Detected

PageView

Microdata Automatically Detected

Facebook Pixel
 Pixel ID: 444588946153193 click to copy
 Troubleshoot Pixel View Analytics

PageView

Accepting New Patients

Hey there, how can I h

3-CV

92. Each time Defendant sends this activity data, it also discloses a patient's personally identifiable information.

94. When accessing the Website, for example, Facebook receives six cookies:

Request Cookies			<input type="checkbox"/> show filtered out request cookies
Name	Value	Domain	
c_user	540...	.facebook.com	
datr	Qtl1...	.facebook.com	
m_page_voice	540...	.facebook.com	
dpr	1.5	.facebook.com	
xs	188...	.facebook.com	
fr	OKF...	.facebook.com	

Figure 7.

95. When a visitor's browser has recently logged out of an account, Facebook compels

the visitor's browser to send a smaller set of cookies²²:

Name	Value	Domain
c_user	540...	.facebook.com
datr	Qt11...	.facebook.com
m_page_voice	540...	.facebook.com
xs	188...	.facebook.com
fr	0YS...	.facebook.com

Figure 8.

96. The fr cookie contains, at least, an encrypted Facebook ID and browser identifier.²³

Facebook, at a minimum, uses the fr cookie to identify users.²⁴

97. At each stage, Defendant also utilized the _fbp cookie, which attaches to a browser as a first-party cookie, and which Facebook uses to identify a browser and a user:²⁵

Name	Value	Domain
_fbp	fb.1.1671026827387.127455195	.rochester.edu

Figure 9. Representation of information shared with Facebook.

98. The fr cookie expires after 90 days unless the visitor's browser logs back into Facebook.²⁶

99. If that happens, the time resets, and another 90 days begins to accrue.²⁷

²² Not pictured here and in the preceding image is the _fbp cookie, which is transmitted as a first-party cookie.

²³ Data Protection Commissioner, *Facebook Ireland Ltd: Report of Re-Audit* (Sept. 21, 2012), p. 33, http://www.europe-v-facebook.org/ODPC_Review.pdf (last visited Dec. 23, 2022).

²⁴ FACEBOOK.COM, COOKIES & OTHER STORAGE TECHNOLOGIES, <https://www.facebook.com/policy/cookies/> (last visited Dec. 23, 2022).

²⁵ *Id.*

²⁶ *Id.*

100. The `_fbp` cookie expires after 90 days unless the visitor's browser accesses the same website.²⁸

101. If that happens, the time resets, and another 90 days begins to accrue.²⁹

102. The Facebook Tracking Pixel uses both first- and third-party cookies. A first-party cookie is “created by the website the user is visiting”—i.e., Defendant.³⁰

103. A third-party cookie is “created by a website with a domain name other than the one the user is currently visiting”—i.e., Facebook.³¹

104. The `_fbp` cookie is always transmitted as a first-party cookie. A duplicate `_fbp` cookie is sometimes sent as a third-party cookie, depending on whether the browser has recently logged into Facebook.

105. Facebook, at a minimum, uses the `fr`, `_fbp`, and `c_user` cookies to link to FIDs and corresponding Facebook profiles.

106. As shown in the above figures, Defendant sent these identifiers with the event data.

107. Plaintiff never consented, agreed, authorized, or otherwise permitted Defendant to disclose her personally identifiable information and protected health information; nor did she

²⁷ Confirmable through developer tools.

²⁸ FACEBOOK.COM, COOKIES & OTHER STORAGE TECHNOLOGIES, <https://www.facebook.com/policy/cookies/>.

²⁹ Confirmable through developer tools.

³⁰ *First-Party Cookie*, PCMAG.COM, <https://www.pcmag.com/encyclopedia/term/first-party-cookie> (last visited Dec. 23, 2022). This is confirmable by using developer tools to inspect a website's cookies and track network activity.

³¹ *Third-Party Cookie*, PCMAG.COM, <https://www.pcmag.com/encyclopedia/term/third-party-cookie> (last visited Dec. 23, 2022). This is also confirmable by tracking network activity.

authorize any assistance with intercepting her communications. Plaintiff was never provided with any written notice that Defendant disclosed its Website users' protected health information, nor was she provided any means of opting out of such disclosures. Despite this, Defendant knowingly disclosed Plaintiff's protected health information to Facebook.

108. By law, Plaintiff is entitled to privacy in her protected health information and confidential communications. Defendant deprived Plaintiff and Class Members of their privacy rights when it: (i) implemented a system that surreptitiously tracked, recorded, and disclosed Plaintiff's and Class Members' confidential communications, personally identifiable information, and protected health information to a third party; (ii) disclosed patients' protected information to Facebook – an unauthorized third-party eavesdropper; and (iii) undertook this pattern of conduct without notifying Plaintiff and Class Members and without obtaining their express written consent. Plaintiff did not discover that Defendant disclosed her personally identifiable information and protected health information to Facebook, and assisted Facebook with intercepting her communications, until approximately December 2022.

Defendant's Privacy Policies & Promises

109. Defendant publishes several privacy policies that represent to patients and visitors to its Website that URM C will keep Private Information private and secure and that it will only disclose PII and PHI provided to it under certain circumstances, ***none of which apply here***.

110. Defendant publishes a Privacy Statement which tells patients that URM C is “committed to protecting your privacy. Any information you provide to us through the URM C website—for example, name, address, and phone number—will never be sold to third parties.”³²

³² <https://www.urmc.rochester.edu/privacy/privacy-statement.aspx> (last visited Dec. 23, 2022).

111. Defendant's Privacy Statement further assures Plaintiffs and Class Members that:

We respect the right to privacy of all patients, families, students, and other visitors to our site. *We do not collect information that would personally identify you unless you choose to provide it. The protected health information that you submit, such as on the appointment request form, is shared only with those people in UPMC who need this information to respond to your question or request.* Information submitted through UPMC online forms may be collected to ensure technical functionality. It will also be utilized to address any inappropriate use of our website. *We do not save protected health information to use for other purposes, nor do we provide it to any other organizations.*

...

*We do not collect information that would personally identify you unless you choose to provide it. We also do not share any visitor's protected health information with any third party unrelated to UPMC, except in situations where we must provide information for legal purposes or investigations, or if so directed by the patient through a proper authorization.*³³

112. Defendant's Notice of Privacy Practices explains Defendant's legal duties with respect to Private Information and the exceptions for when Defendant can lawfully use and disclose Plaintiff's and Class Members' Private Information in the following ways:

- For treatment;
- For health care operations;
- To business associates ("Our contracts with them require that they protect the privacy of your health information");
- For appointment reminders;
- For health-related benefits and treatment activities;
- For fundraising activities;
- For the patient information directory;
- To individuals involved in patient care or payment for patient care;
- For research;
- Incidental disclosures ("Disclosures of your information may occur during or as an unavoidable result of otherwise permissible uses or disclosures of your health information. For example, during the course of your treatment, other patients in the area may see or overhear discussion of your health information despite using reasonable safeguards");
- To personal representatives;
- For limited marketing purposes ("We may use your information for certain limited marketing purposes, such as face-to-face communication. For other marketing

³³ *Id.* (emphasis added).

- activities we will obtain your authorization”);
- To comply with the law;
 - To address workers’ compensation, law enforcement and other government requests;
 - For public health purposes including to avert a serious or imminent threat to health and safety;
 - For organ and tissue donations;
 - To coroners, medical examiners and funeral directors;
 - To correctional institutions where patient is an inmate, in limited circumstances;
 - To schools (student immunization information);
 - To respond to lawsuits and other legal actions.³⁴

113. Defendant further acknowledges that it may only sell patients’ protected health information without their written authorization only in very limited circumstances, “such as if the covered entity is sold.”³⁵

114. Defendant also acknowledges the following:

We are required by law to:

- Make sure that medical information that identifies you is kept private;
- Give you this Notice of our legal duties and privacy practices with respect to medical information about you; and
- Follow the terms of this Notice.

...

You have the right to be notified of a breach of your unsecured protected health information, with a few limited exceptions. A breach is defined as unauthorized acquisition, access, use or disclosure of protected health information in a manner not permitted, unless there is a low probability that the privacy or security of your protected health information has been compromised.

...

Other uses and disclosures of medical information not covered by this Notice or the laws that apply to us will be made only with your written authorization.³⁶

³⁴

<https://www.urmc.rochester.edu/MediaLibraries/URMCMedia/privacy/documents/NoticeofPrivacyPracticesHIPAA.pdf> (last visited Dec. 23, 2022).

³⁵ *Id.*

³⁶ *Id.*

115. While Defendant's Privacy Statement discloses that it uses "Google AdWords remarketing service to advertise UPMC services to previous visitors to our site," it also states that "[a]ny data collected will be used in accordance with our privacy policy and Google's privacy policy."³⁷ Defendant's privacy policies do **not** permit Defendant to use and disclose Plaintiff's and Class Members' Private Information for marketing purposes.

116. Defendant's assurances that it will keep patients' Private Information confidential and secure, are false.

117. Defendant conceals its use of Facebook Pixels to track patients' personally identifiable information, even when it discusses its use of internet analytical tools:

The website uses Web analytics software to track visitor activity and to better understand how the website can be improved. ***The website does not allow any third party to track or collect personally identifiable information from users. If personally identifiable data is collected, (see the Protected Health Information section) none of that data will be associated with any other data gathered during the use of this website.***

We may provide third parties with aggregate statistics about our visitors, traffic patterns and related site information. These data reflect site-usage patterns gathered during visits to our website, but ***they do not contain behavioral or identifying information about any individual user unless that user has given us permission to share that information.***³⁸

118. Defendant admits that it collects patients' IP addresses, but falsely states that this is "not truly personally identifiable information."³⁹

119. Defendant also falsely states that "first party cookies" which it uses to "collect information about visitors to our site . . . are never associated with specific personal identities."

³⁷ <https://www.upmc.rochester.edu/privacy/privacy-statement.aspx>

³⁸ *Id.* (emphasis added).

³⁹ *See id.* Under HIPAA, an IP address is considered personally identifiable information. *See* 45 C.F.R. § 164.514 (2); *see also* discussion *infra*.

120. Defendant violated its own privacy policies by unlawfully intercepting and disclosing Plaintiff's and Class Members' Private Information to Facebook and third parties without adequately disclosing that Defendant shared Private Information with third parties and without acquiring the specific patients' consent or authorization to share the Private Information.

Defendant Violated HIPAA Standards

121. Under federal law, a healthcare provider may not disclose personally identifiable, non-public medical information about a patient, a potential patient, or household member of a patient for marketing purposes without the patients' express written authorization.⁴⁰

122. Guidance from the United States Department of Health and Human Services instructs healthcare providers that patient status alone is protected by HIPAA.

123. In Guidance regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act Privacy Rule, the Department instructs:

Identifying information alone, such as personal names, residential addresses, or phone numbers, would not necessarily be designated as PHI. For instance, if such information was reported as part of a publicly accessible data source, such as a phone book, then this information would not be PHI because it is not related to health data... If such information was listed with health condition, health care provision, or payment data, such as an indication that the individual was treated at a certain clinic, then this information would be PHI.⁴¹

124. In its guidance for Marketing, the Department further instructs:

The HIPAA Privacy Rule gives individuals important controls over whether and how their protected health information is used and

⁴⁰ HIPAA, 42 U.S.C. § 1320; 45 C.F.R. §§ 164.502; 164.508(a)(3), 164.514(b)(2)(i).

⁴¹ https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/De-identification/hhs_deid_guidance.pdf (last visited Dec. 23, 2022).

disclosed for marketing purposes. With limited exceptions, the Rule requires an individual's written authorization before a use or disclosure of his or her protected health information can be made for marketing. ... Simply put, a covered entity may not sell protected health information to a business associate or any other third party for that party's own purposes. Moreover, *covered entities may not sell lists of patients to third parties* without obtaining authorization from each person on the list. (Emphasis added).⁴²

Defendant Violated Industry Standards

125. A medical provider's duty of confidentiality is embedded in the physician-patient and hospital-patient relationship, it is a cardinal rule.

126. The American Medical Association's ("AMA") Code of Medical Ethics contains numerous rules protecting the privacy of patient data and communications.

127. AMA Code of Ethics Opinion 3.1.1 provides:

Protecting information gathered in association with the care of the patient is a core value in health care... Patient privacy encompasses a number of aspects, including, ... personal data (informational privacy)[.]

128. AMA Code of Medical Ethics Opinion 3.2.4 provides:

Information gathered and recorded in association with the care of the patient is confidential. Patients are entitled to expect that the sensitive personal information they divulge will be used solely to enable their physician to most effectively provide needed services. Disclosing information for commercial purposes without consent undermines trust, violates principles of informed consent and confidentiality, and may harm the integrity of the patient-physician relationship. Physicians who propose to permit third-party access to specific patient information for commercial purposes should: (a) Only provide data that has been de-identified. [and] (b) Fully inform each patient whose record would be involved (or the patient's authorized surrogate when the individual lacks decision-making capacity about the purposes for which access would be granted.

⁴² <https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/marketing.pdf> (last visited Dec. 23, 2022).

129. AMA Code of Medical Ethics Opinion 3.3.2 provides:

Information gathered and recorded in association with the care of a patient is confidential, regardless of the form in which it is collected or stored. Physicians who collect or store patient information electronically...must: (c) Release patient information only in keeping with ethics guidelines for confidentiality.⁴³

Defendant Violated New York Standards

130. New York State has long been a national leader in protecting the confidentiality of personal medical information. New York State law has strict privacy standards for medical records. Unlike HIPAA, New York requires patient consent before a physician can disclose an individual's medical information to another treating physician.⁴⁴ It also limits disclosure to immediately relevant information.⁴⁵

131. Even stronger protections restrict the release of certain especially sensitive information regarding genetic tests,⁴⁶ mental health,⁴⁷ medical treatment of adolescents,⁴⁸ sexually transmitted infections,⁴⁹ and HIV.⁵⁰

⁴³ <https://www.ama-assn.org/sites/ama-assn.org/files/corp/media-browser/code-of-medical-ethics-chapter-3.pdf> (last visited December 23, 2022).

⁴⁴ See New York Public Health Law § 18(6).

⁴⁵ *Id.*

⁴⁶ See New York Civil Rights Law § 79-l.

⁴⁷ *Id.* at § 79-j; New York Public Health Law § 18(1)(e); Mental Hygiene Law § 33.13.

⁴⁸ Barriers to the Exchange of Pediatric Health Information, NY eHealth Collaborative Privacy & Security Minor Consent Tiger Team, pages 7-8 (July 2, 2010) (describing numerous state law provisions and state and federal case law that create confidentiality rights for minors seeking health care on their own).

⁴⁹ See New York Public Health Law Chapter 45, § 2306.

⁵⁰ See New York Public Health Law Chapter 45, Article 27-F.

132. New York State Department of Health regulations governing hospitals impose significant privacy and security standards relating to medical records, patient rights, and medical staff by-laws. With respect to medical records, a hospital must ensure the confidentiality of patient records and release records or information from records “only to hospital staff involved in treating the patient and individuals as permitted by Federal and State laws.”⁵¹ This provision has been interpreted to require hospitals to obtain consent from the patient prior to disclosing medical records to an outside entity, even for treatment or reimbursement purposes.⁵² A hospital must also institute safeguards to protect the security of medical records, including a system “to ensure the integrity of the authentication and protect the security of all transmissions, records and record entries” as well as implement policies to ensure the security of electronic or computer equipment from unwarranted access.⁵³

Plaintiff’s & Class Members’ Expectation of Privacy

133. Plaintiff and Class Members were aware of Defendant’s duty of confidentiality when they sought medical services from Defendant.

134. Indeed, at all times when Plaintiff and Class Members provided their PII and PHI to Defendant, they each had a reasonable expectation that the information would remain private, and that Defendant would not share the Private Information with third parties for a commercial purpose unrelated to patient care.

IP Addresses are Personally Identifiable Information

135. In addition to patient status, address, medical conditions, treatment, specific

⁵¹ 10 NYCRR § 405.10 (a)(6).

⁵² See *Williams v. Roosevelt Hospital*, 66 N.Y.2d 391 (1985).

⁵³ 10 NYCRR § 405.10 (a)(2).

providers, appointment information, and patient's unique and persistent Facebook ID, Defendant improperly disclosed patients' computer IP addresses to Facebook through the use of the Pixel.

136. An IP address is a number that identifies the address of a device connected to the Internet.

137. IP addresses are used to identify and route communications on the Internet.

138. IP addresses of individual Internet users are used by Internet service providers, Websites, and third-party tracking companies to facilitate and track Internet communications.

139. Facebook tracks every IP address ever associated with a Facebook user.

140. Google also tracks IP addresses associated with Internet users.

141. Facebook, Google, and other third-party marketing companies track IP addresses for use of tracking and targeting individual homes and their occupants with advertising by using IP addresses.

142. Under HIPAA, an IP address is considered personally identifiable information:

- a. HIPAA defines personally identifiable information to include "any unique identifying number, characteristic or code" and specifically lists the example of IP addresses. *See* 45 C.F.R. § 164.514 (2).
- b. HIPAA further declares information as personally identifiable where the covered entity has "actual knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the information." 45 C.F.R. § 164.514(2)(ii); *See also*, 45 C.F.R. § 164.514(b)(2)(i)(O).

143. Consequently, Defendant's disclosure of patients' IP addresses violated HIPAA and industry privacy standards.

Defendant was Enriched & Benefitted from the Use of The Pixel & Unauthorized Disclosures

144. The sole purpose of the use of the Facebook Pixel on Defendant's Website was marketing and profits.

145. In exchange for disclosing the personally identifiable information of its patients, Defendant is compensated by Facebook in the form of enhanced advertising services and more cost-efficient marketing on Facebook.

146. Upon information and belief, Defendant was advertising its services on Facebook, and the Pixel was used to "help [Defendant] understand the success of [its] advertisement efforts on Facebook."

147. Retargeting is a form of online marketing that targets users with ads based on their previous Internet communications and interactions.

148. Upon information and belief, Defendant re-targeted patients and potential patients to get more patients to use its services.

149. By utilizing the Pixel, the cost of advertising and retargeting was reduced, thereby benefitting Defendant.

Representative Plaintiff Carol Kane's Experiences

150. As a condition of receiving Defendant's services, Plaintiff Kane disclosed her Private Information to Defendant as recently as November 2022.

151. Plaintiff Kane accessed Defendant's Website on her phone and computer to receive healthcare services from Defendant and at Defendant's direction.

152. Plaintiff Kane scheduled doctor's appointments for herself via the Defendant's Website.

153. Plaintiff Kane has used and continues to use the same devices to maintain and access an active Facebook account throughout the relevant period in this case.

154. Plaintiff Kane reasonably expected that her communications with Defendant via the Website were confidential, solely between herself and Defendant, and that such communications would not be transmitted to or intercepted by a third party.

155. Plaintiff Kane provided her Private Information to Defendant and trusted that the information would be safeguarded according to Defendant's policies and state and federal law.

156. As described herein, Defendant worked along with Facebook to intercept Plaintiff Kane's communications, including those that contained Private and confidential information.

157. Defendant willfully facilitated these interceptions without Plaintiff Kane's knowledge, consent, or express written authorization.

158. Defendant transmitted to Facebook Plaintiff Kane's Facebook ID, computer IP address, location, and information such as treatment sought, appointment type, physician selected, and button/menu selections.

159. By doing so without Plaintiff Kane's consent, Defendant breached Plaintiff Kane's right to privacy and unlawfully disclosed Plaintiff Kane's Private Information.

160. Defendant did not inform Plaintiff Kane that it had shared her Private Information with Facebook.

161. Plaintiff Kane suffered damages in, *inter alia*, the form of (i) invasion of privacy; (ii) violation of confidentiality of her Private Information; (iii) loss of benefit of the bargain; (iv) diminution of value of the Private Information; (v) statutory damages; and (vi) the continued and ongoing risk to her Private Information.

162. Plaintiff Kane has a continuing interest in ensuring that her Private Information

is protected and safeguarded from future unauthorized disclosure.

TOLLING

163. Any applicable statute of limitations has been tolled by the “delayed discovery” rule. Plaintiff did not know (and had no way of knowing) that Plaintiff’s PII and PHI was intercepted and unlawfully disclosed because Defendant kept this information secret.

CLASS ACTION ALLEGATIONS

164. Plaintiff Kane brings this action on behalf of herself and on behalf of all other persons similarly situated (“the Class”) pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

165. The Nationwide Class that Plaintiffs seek to represent is defined as follows:

All individuals residing in the United States whose Private Information was disclosed to a third party without authorization or consent through the Pixel on Defendant’s Website.

166. Excluded from the Class are Defendant, its agents, affiliates, parents, subsidiaries, any entity in which Defendant has a controlling interest, any Defendant officer or director, any successor or assign, and any Judge who adjudicates this case, including their staff and immediate family.

167. Plaintiff reserves the right to modify or amend the definition of the proposed classes before the Court determines whether certification is appropriate.

168. **Numerosity, Fed. R. Civ. P. 23(a)(1).** The Nationwide Class members are so numerous that joinder of all members is impracticable. Upon information and belief, there are over one million individuals whose PII and PHI may have been improperly accessed by Facebook, and the Class is identifiable within Defendant’s records.

169. **Commonality & Predominance, Fed. R. Civ. P. 23(a)(2) and (b)(3).** Questions

of law and fact common to the Classes exist and predominate over any questions affecting only individual Class Members. These include:

- a. Whether and to what extent Defendant had a duty to protect the PII and PHI of Plaintiff and Class Members;
- b. Whether Defendant had duties not to disclose the PII and PHI of Plaintiff and Class Members to unauthorized third parties;
- c. Whether Defendant violated its privacy policy by disclosing the PII and PHI of Plaintiff and Class Members to Facebook, Meta, and/or additional third parties.
- d. Whether Defendant adequately, promptly, and accurately informed Plaintiff and Class Members that their PII and PHI would be disclosed to third parties;
- e. Whether Defendant violated the law by failing to promptly notify Plaintiff and Class Members that their PII and PHI had been compromised;
- f. Whether Defendant adequately addressed and fixed the practices which permitted the disclosure of patient PHI and PII;
- g. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII and PHI of Plaintiff and Class Members;
- h. Whether Defendant violated the consumer protection statutes invoked herein;
- i. Whether Plaintiff and Class Members are entitled to actual, consequential, and/or nominal damages as a result of Defendant's wrongful conduct;
- j. Whether Defendant knowingly made false representations as to its data security and/or privacy policy practices;
- k. Whether Defendant knowingly omitted material representations with respect to its data security and/or privacy policy practices; and

1. Whether Plaintiff and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Defendant's disclosure of their PII and PHI.

170. **Typicality, Fed. R. Civ. P. 23(a)(3).** Plaintiff's claims are typical of those of other Class Members because all had their PII and PHI compromised as a result of Defendant's incorporation of the Facebook Pixel, due to Defendant's misfeasance.

171. **Adequacy, Fed. R. Civ. P. 23(a)(4).** Plaintiff will fairly and adequately represent and protect the interests of the Class Members in that Plaintiff has no disabling conflicts of interest that would be antagonistic to those of the other Members of the Class. Plaintiff seeks no relief that is antagonistic or adverse to the Members of the Class and the infringement of the rights and the damages Plaintiff has suffered are typical of other Class Members. Plaintiff has also retained counsel experienced in complex class action litigation, and Plaintiff intends to prosecute this action vigorously.

172. **Superiority and Manageability, Fed. R. Civ. P. 23(b)(3).** Class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Defendant. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

173. **Policies Generally Applicable to the Class.** This class action is also appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Class as a whole. Defendant's policies challenged herein apply to and affect Class Members uniformly and Plaintiff's challenge of these policies hinges on Defendant's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff.

174. The nature of this action and the nature of laws available to Plaintiff and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiff and Class Members for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since they would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiff was exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

175. The litigation of the claims brought herein is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrate that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

176. **Ascertainability & Notice.** Membership in the Class can be determined by objective records maintained by Defendant and adequate notice can be given to Class Members

directly using information maintained in Defendant's records.

177. **Class-wide Injunctive Relief, Fed. R. Civ. P. 23(b)(2).** Unless a Class-wide injunction is issued, Defendant may continue in its failure to properly secure the Private Information of Class Members, Defendant may continue to refuse to provide proper notification to Class Members regarding the practices complained of herein, and Defendant may continue to act unlawfully as set forth in this Complaint as Defendant has acted or refused to act on grounds generally applicable to the Class and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class Members as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

178. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

- a. Whether Defendant owed a legal duty to not disclose Plaintiff's and Class Members' Private Information;
- b. Whether Defendant owed a legal duty to not disclose Plaintiff's and Class Members' Private Information with respect to Defendant's privacy policy;
- c. Whether Defendant breached a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their Private Information;
- d. Whether Defendant failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;
- e. Whether Defendant adequately and accurately informed Plaintiff and Class

Members that their Private Information would be disclosed to third parties;

- f. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information disclosed to third parties;
- g. Whether Class Members are entitled to actual, consequential, and/or nominal damages, and/or injunctive relief as a result of Defendant's wrongful conduct.

179. Plaintiff reserves the right to amend or modify the Class definition as this case progresses.

NEW YORK LAW SHOULD APPLY TO PLAINTIFF AND THE CLASS AS A WHOLE

180. The State of New York has a significant interest in regulating the conduct of businesses operating within its borders.

181. New York, which seeks to protect the rights and interests of New Yorkers and all residents and citizens of the United States against a company headquartered and doing business in New York, has a greater interest in the claims of Plaintiff and the Class than any other state and is most intimately concerned with the claims and outcome of this litigation.

182. The principal place of business and headquarters of UPMC, located in Rochester, New York, is the "nerve center" of its business activities – the place where its high-level officers direct, control and coordinate Defendant's activities, including major policy decisions.

183. Defendant's actions and corporate decisions surrounding the allegations made in the Complaint were made from and in New York.

184. Defendant's breaches of duty to Plaintiff and Class Members emanated from New York.

185. Application of New York law to the Class with respect to Plaintiff's and Class

Members' claims is neither arbitrary nor fundamentally unfair because New York has significant contacts and a significant aggregation of contacts that create a state interest in the claims of Plaintiff and the Class.

186. Under New York's choice of law principles, which are applicable to this action, the common law of New York applies to the nationwide common law claims of all Class Members.

187. Additionally, given New York's significant interest in regulating the conduct of businesses operating within its borders, and that New York has the most significant relationship to Defendant, as it is headquartered in New York, and its executives and officers are located and made decisions which have given rise to the allegations and claims asserted herein, in New York, there is no conflict in applying New York law to non-resident consumers such as some of the potential Class Members.

CLAIMS

COUNT I

INVASION OF PRIVACY (On Behalf of Plaintiff & the Class)

188. Plaintiff and Class Members repeat and re-allege each and every allegation in the Complaint as if fully set forth herein.

189. Plaintiff brings this claim individually and on behalf of the members of the proposed Class against Defendant.

190. Plaintiff and Class Members had a reasonable expectation of privacy in their communications with Defendant via its Website and the communications platforms and services therein.

191. Plaintiff and Class Members communicated sensitive and protected medical

information and individually identifiable information that they intended for only Defendant to receive and that they understood Defendant would keep private.

192. Defendant's disclosure of the substance and nature of those communications to third parties without the knowledge and consent of Plaintiffs and Class members is an intentional intrusion on Plaintiff's and Class members' solitude or seclusion.

193. Plaintiff and Class members had a reasonable expectation of privacy given Defendant's representations, its Notice of Privacy Practices and Privacy Statement.

194. Moreover, Plaintiff and Class members have a general expectation that their communications regarding healthcare with their healthcare providers will kept confidential. Defendant's disclosure of private medical information coupled with individually identifying information is highly offensive to the reasonable person.

195. As a result of Defendant's actions, Plaintiff and Class members have suffered harm and injury, including but not limited to an invasion of their privacy rights.

196. Plaintiff and Class members have been damaged as a direct and proximate result of Defendant's invasion of their privacy and are entitled to just compensation, including monetary damages.

197. Plaintiff and Class members seek appropriate relief for that injury, including but not limited to damages that will reasonably compensate Plaintiff and Class members for the harm to their privacy interests as a result of its intrusions upon Plaintiff's and Class members' privacy.

198. Plaintiff and Class members are also entitled to punitive damages resulting from the malicious, willful, and intentional nature of Defendant's actions, directed at injuring Plaintiff and Class members in conscious disregard of their rights. Such damages are needed to deter Defendant from engaging in such conduct in the future.

199. Plaintiff also seeks such other relief as the Court may deem just and proper.

COUNT II

BREACH OF CONTRACT **(On behalf of Plaintiff & the Class)**

200. Plaintiff and Class Members repeat and re-allege each and every allegation in the Complaint as if fully set forth herein.

201. Defendant required Plaintiff and Class Members to provide their Private Information, including names, email addresses, phone numbers, computer IP addresses, appointment information, and other content submitted into Defendant's Website as a condition of their receiving healthcare services.

202. As a condition of utilizing Defendant's digital platforms and receiving services from Defendant, Plaintiff and Class Members provided their Private Information and compensation for their medical care. In so doing, Plaintiff and Class Members entered into contracts with Defendant by which Defendant agreed to safeguard and protect such information, in its Privacy Policies and elsewhere, to keep such information secure and confidential, and to timely and accurately notify Plaintiff and Class Members if their data had been breached and compromised or stolen.

203. Plaintiff and Class Members fully performed their obligations under the contract with Defendant.

204. Defendant's relevant privacy policies and representations require it to take appropriate steps to safeguard the Private Information entrusted to it by the Plaintiff and Class Members.

205. Defendant breached these agreements, which directly and/or proximately caused

Plaintiff and Class Members to suffer damages, including nominal damages.

206. Defendant breached the contracts it made with Plaintiff and Class Members by failing to safeguard and protect their Private Information, and by failing to provide timely and accurate notice to them that the Private Information was compromised as a result of the Defendant sharing the Private Information with third parties without proper authorization.

207. As a direct and proximate result of Defendant's above-described breach of contract, Plaintiff and Class Members have suffered (and will continue to suffer) the compromise and disclosure of their Private Information and identities.

208. As a direct and proximate result of Defendant's above-described breach of contract, Plaintiff and Class Members are entitled to recover actual, consequential, and nominal damages.

COUNT III

BREACH OF FIDUCIARY DUTY **(On Behalf of Plaintiff & the Class)**

209. Plaintiff re-alleges and incorporates by reference all other paragraphs in the Complaint as if fully set forth herein.

210. A relationship existed between Plaintiff and Class Members on the one hand and Defendant on the other in which Plaintiff and Class Members put their trust in Defendant to protect the Private Information of Plaintiff and Class Members, and Defendant accepted that trust.

211. Defendant breached the fiduciary duty that it owed to Plaintiff and Class Members by failing to act with the utmost good faith, fairness, and honesty, failing to act with the highest and finest loyalty, and failing to protect, and intentionally disclosing, the Private Information of Plaintiff and Class Members.

212. Defendant's breach of fiduciary duty was a legal cause of damage to Plaintiff and

Class Members.

213. But for Defendant's breach of fiduciary duty, the damage to Plaintiff and Class Members would not have occurred.

214. Defendant's breach of fiduciary duty contributed substantially to producing the damage to Plaintiff and Class Members.

215. As a direct and proximate result of Defendant's breach of fiduciary duty, Plaintiff and Class Members are entitled to and do demand actual, consequential, and nominal damages, injunctive relief, and all other relief allowed by law.

COUNT IV

UNJUST ENRICHMENT **(On behalf of Plaintiff & the Class)**

216. Plaintiff repeats and re-alleges each and every allegation contained in the Complaint as if fully set forth herein.

217. Defendant benefitted from Plaintiff and Class Members and unjustly retained those benefits at their expense.

218. Plaintiff and Class Members conferred a benefit upon Defendant in the form of Private Information that Defendant collected from Plaintiff and Class Members, without authorization and proper compensation. Defendant consciously collected and used this information for its own gain, providing Defendant with economic, intangible, and other benefits, including substantial monetary compensation.

219. Defendant unjustly retained those benefits at the expense of Plaintiff and Class Members because Defendant's conduct damaged Plaintiff and Class Members, all without providing any commensurate compensation to Plaintiff and Class Members.

220. The benefits that Defendant derived from Plaintiff and Class Members was not offered by Plaintiff and Class Members gratuitously and rightly belongs to Plaintiff and Class Members. It would be inequitable under unjust enrichment principles in New York and every other state for Defendant to be permitted to retain any of the profit or other benefits wrongly derived from the unfair and unconscionable methods, acts, and trade practices alleged in this Complaint.

221. Defendant should be compelled to disgorge into a common fund for the benefit of Plaintiff and Class Members all unlawful or inequitable proceeds that Defendant received, and such other relief as the Court may deem just and proper.

COUNT V

BREACH OF IMPLIED CONTRACT (On behalf of Plaintiff & the Class)

222. Plaintiff repeats and re-alleges each and every allegation contained in the Complaint as if fully set forth herein.

223. When Plaintiff and Class Members provided their user data to Defendant in exchange for services, they entered an implied contract pursuant to which Defendant agreed to safeguard and not disclose their Private Information without consent.

224. Plaintiff and Class Members accepted Defendant's offers and provided their Private Information to Defendant.

225. Plaintiff and Class Members would not have entrusted Defendant with their Private Information in the absence of an implied contract between them and Defendant obligating them not to disclose this Private Information without consent.

226. Defendant breached these implied contracts by disclosing Plaintiff's and Class

Members' Private Information to a third party, i.e., Facebook.

227. As a direct and proximate result of Defendant's breaches of these implied contracts, Plaintiff and Class Members sustained damages as alleged herein. Plaintiff and Class Members would not have used Defendant's services, or would have paid substantially for these services, had they known their Private Information would be disclosed.

228. Plaintiff and Class Members are entitled to compensatory and consequential damages as a result of Defendant's breach of implied contract.

COUNT VI

VIOLATION OF THE NEW YORK DECEPTIVE TRADE PRACTICES ACT (New York Gen. Bus. Law § 349) (On Behalf of Plaintiff & the Class)

229. Plaintiff re-alleges and incorporates by reference all other paragraphs in the Complaint as if fully set forth herein.

230. By the acts and conduct alleged herein, Defendant committed unfair or deceptive acts and practices by:

- a. promising to maintain the privacy and security of Plaintiff's and Class Members' protected health information as required by law;
- b. installing the Facebook Pixel to operate as intended and transmit Plaintiff's and Class Members' Private Information without their authorization to Facebook;
- c. failing to disclose or omitting material facts to Plaintiff and Class Members regarding the disclosure of their Private Information to Facebook;
- d. failing to take proper action to ensure the Pixel was configured to prevent unlawful disclosure of Plaintiff's and Class Members' Private Information;
- e. unlawfully disclosing Plaintiff's and Class Members' Private Information to Facebook.

231. These unfair acts and practices violated duties imposed by laws, including but not

limited to, the Federal Trade Commission Act, HIPAA, and NY GBL § 349.

232. Defendant's actions also constitute deceptive and unfair acts or practices because Defendant knew it failed to disclose to Plaintiff and Class Members that their healthcare related communications via the Website would be disclosed to Facebook.

233. Defendant's actions also constitute deceptive and unfair acts or practices because Defendant intended that Plaintiff and Class Members rely on its deceptive and unfair acts and practices and the concealment and omission of material facts in connection with Defendant's offering of goods and services.

234. Specifically, Defendant was aware that Plaintiff and Class Members depended and relied upon it to keep their communications confidential and Defendant instead disclosed that information to Facebook.

235. In addition, Defendant's material failure to disclose that Defendant collects Plaintiff's and Class Members' Private Information for marketing purposes with Facebook constitutes an unfair act or practice prohibited by the NY GBL § 349. Defendant's actions were immoral, unethical, and unscrupulous.

236. Plaintiff had reasonable expectations of privacy in her communications exchanged with Defendant, including communications exchanged at <https://www.urmc.rochester.edu/>.

237. Plaintiff's reasonable expectations of privacy in the communications exchanged with Defendant were further buttressed by Defendant's express promises in its Notice of Privacy Statement and HIPAA Privacy Notice.

238. Contrary to its duties as a medical provider and its express promises of confidentiality, Defendant deployed the Pixel to disclose and transmit Plaintiff's personally identifiable, non-public medical information, and the contents of her communications exchanged

with Defendant to third parties, i.e., Facebook.

239. Defendant's disclosures of Plaintiff's and Class Members' Private Information were made without their knowledge, consent, or authorization, and were unprivileged.

240. The harm arising from a breach of provider-patient confidentiality includes erosion of the essential confidential relationship between the healthcare provider and the patient.

241. Defendant willfully, knowingly, intentionally, and voluntarily engaged in the aforementioned acts when it incorporated the Facebook Pixel with knowledge of the Pixel's purpose and functionality.

242. The harm described herein could not have been avoided by Plaintiff and Class Members through the exercise of ordinary diligence.

243. As a result of Defendant's wrongful conduct, Plaintiff was injured in that she never would have provided her PII and PHI to Defendant, or purchased Defendant's services, had she known or been told that Defendant shared her confidential and sensitive Private Information with Facebook.

244. As a direct and proximate result of Defendant's multiple, separate violations of the NY GBL § 349, Plaintiff and Class Member have suffered harm, including financial losses related to the payments or services made to Defendant that Plaintiff and Class Members would not have made had they known of Defendant's disclosure of their PII and PHI to Facebook; lost control over the value of their PII and PHI; and other harm resulting from the unauthorized use or threat of unauthorized use of their PII and PHI, including for unwanted solicitations or marketing, entitling them to damages in an amount to be proven at trial.

245. Defendant's acts, practices and omissions were done in the course of Defendant's business of furnishing healthcare-related services to consumers in the State of New York.

246. Plaintiff brings this action on behalf of herself and Class Members for the relief requested above and for the public benefit to promote the public interests in the provision of truthful, fair information to allow consumers to make informed purchasing decisions and to protect Plaintiff, Class Members and the public from Defendant's unfair, deceptive and unlawful practices. Defendant's wrongful conduct as alleged in this Complaint has had widespread impact on the public at large.

247. As a result, Plaintiffs and the Class Members are entitled to damages in an amount to be determined at trial, along with their costs and attorneys' fees incurred in this action.

COUNT VII

VIOLATIONS OF ELECTRONIC COMMUNICATIONS PRIVACY ACT ("ECPA")

18 U.S.C. § 2511(1) *et seq.*

UNAUTHORIZED INTERCEPTION, USE, AND DISCLOSURE

(On Behalf of Plaintiff & the Class)

248. Plaintiff repeats and re-alleges each and every allegation contained in the Complaint as if fully set forth herein.

249. The ECPA protects both sending and receipt of communications.

250. 18 U.S.C. § 2520(a) provides a private right of action to any person whose wire or electronic communications are intercepted, disclosed, or intentionally used in violation of Chapter 119.

251. The transmissions of Plaintiff's PII and PHI to Defendant's Website qualifies as a "communication" under the ECPA's definition of 18 U.S.C. § 2510(12).

252. **Electronic Communications.** The transmission of PII and PHI between Plaintiff and Class Members and Defendant's Website with which they chose to exchange communications are "transfer[s] of signs, signals, writing, ...data, [and] intelligence of [some] nature transmitted in

whole or in part by a wire, radio, electromagnetic, photoelectronic, or photooptical system that affects interstate commerce” and are therefore “electronic communications” within the meaning of 18 U.S.C. § 2510(2).

253. **Content.** The ECPA defines content, when used with respect to electronic communications, to “include [] *any* information concerning the substance, purport, or meaning of that communication.” 18 U.S.C. § 2510(8).

254. **Interception.** The ECPA defines the interception as the “acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device” and “contents...include any information concerning the substance, purport, or meaning of that communication.” 18 U.S.C. § 2510(4), (8).

255. **Electronic, Mechanical, or Other Device.** The ECPA defines “electronic, mechanical, or other device” as “any device...which can be used to intercept a[n]...electronic communication[.]” 18 U.S.C. § 2510(5). The following constitute “devices” within the meaning of 18 U.S.C. § 2510(5):

- a. Plaintiff’s and Class Members’ browsers;
- b. Plaintiff’s and Class Members’ computing devices;
- c. Defendant’s web-servers;
- d. Defendant’s Website; and
- e. The Pixel code deployed by Defendant to effectuate the sending and acquisition of patient communications.

256. By utilizing and embedding the Pixel on its Website, Defendant intentionally intercepted, endeavored to intercept, and procured another person to intercept, the electronic communications of Plaintiff and Class Members, in violation of 18 U.S.C.

§ 2511(1)(a).

257. Specifically, Defendant intercepted Plaintiff's and Class Members' electronic communications via the Pixel, which tracked, stored, and unlawfully disclosed Plaintiff's and Class Members' PII to Facebook.

258. Defendant's intercepted communications include, but are not limited to, communications to/from Plaintiff's and Class Members' regarding PII and PHI, treatment, medication, and scheduling.

259. By intentionally disclosing or endeavoring to disclose the electronic communications of Plaintiff and Class Members to affiliates and other third parties, while knowing or having reason to know that the information was obtained through the interception of an electronic communication in violation of 18 U.S.C. § 2511(1)(a), Defendant violated 18 U.S.C. § 2511(1)(c).

260. By intentionally using, or endeavoring to use, the contents of the electronic communications of Plaintiff and Class Members, while knowing or having reason to know that the information was obtained through the interception of an electronic communication in violation of 18 U.S.C. § 2511(1)(a), Defendant violated 18 U.S.C. § 2511(1)(d).

261. **Unauthorized Purpose.** Defendant intentionally intercepted the contents of Plaintiff's and Class Members' electronic communications for the purpose of committing a tortious act in violation of the Constitution or laws of the United States or of any State – namely, invasion of privacy, among others.

262. Defendant intentionally used the wire or electronic communications to increase its profit margins. Defendant specifically used the Pixel to track and utilize Plaintiff's and Class Members' PII and PHI for financial gain.

263. Defendant was not acting under color of law to intercept Plaintiff and Class Member's wire or electronic communication.

264. Plaintiff and Class Members did not authorize Defendant to acquire the content of their communications for purposes of invading Plaintiff's privacy via the Pixel tracking code.

265. Any purported consent that Defendant received from Plaintiff and Class Members was not valid.

266. In sending and in acquiring the content of Plaintiff's and Class Members' communications relating to the browsing of Defendant's Website, Defendant's purpose was tortious, criminal, and designed to violate federal and state legal provisions, including as described above the following: (i) a knowing intrusion into a private, place, conversation, or matter that would be highly offensive to a reasonable person; and (ii) violation of NY GBL § 349.

COUNT VIII

**VIOLATION OF ELECTRONIC COMMUNICATIONS PRIVACY ACT
UNAUTHORIZED DIVULGENCE BY ELECTRONIC COMMUNICATIONS SERVICE
18 U.S. Code § 2511(3)(a)
(On Behalf of Plaintiff & the Class)**

267. Plaintiff repeats and re-alleges each and every allegation contained in the Complaint as if fully set forth herein.

268. The ECPA statute provides that "a person or entity providing an electronic communication service to the public shall not intentionally divulge the contents of any communication (other than one to such person or entity, or an agent thereof) while in transmission on that service to any person or entity other than an addressee or intended recipient of such communication or an agent of such addressee or intended recipient." 18 U.S.C. § 2511(3)(a).

269. **Electronic Communication Service.** An "electronic communication service" is

defined as “any service which provides to users thereof the ability to send or receive wire or electronic communications.” 18 U.S.C. § 2510(15).

270. Defendant’s Website is an electronic communication service which provides to users thereof the ability to send or receive electronic communications. In the absence of Defendant’s website, internet users could not send or receive communications regarding Plaintiff’s and Class Members’ PII and PHI.

271. **Intentional Divulgence.** Defendant intentionally designed the Pixel tracking and was or should have been aware that, if misconfigured, it could divulge Plaintiff’s and Class Members’ PII and PHI.

272. **While in Transmission.** Upon information and belief, Defendant’s divulgence of the contents of Plaintiff’s and Class Members’ communications was contemporaneous with their exchange with Defendant’s Website, to which they directed their communications.

273. Defendant divulged the contents of Plaintiff’s and Class Members’ electronic communications without authorization. Defendant divulged the contents of Plaintiff’s and Class Members’ communications to Facebook without Plaintiff’s and Class Members’ consent and/or authorization.

274. **Exceptions do not apply.** In addition to the exception for communications directly to an electronic communications service (“ECS”)⁵⁴ or an agent of an ECS, the ECPA states that “[a] person or entity providing electronic communication service to the public may divulge the contents of any such communication”

a. “as otherwise authorized in section 2511(2)(a) or 2517 of this title;”

⁵⁴ An ECS is “any service which provides to users thereof the ability to send or receive wire or electronic communications.” 18 U.S.C. § 2510(15).

- b. “with the lawful consent of the originator or any addressee or intended recipient of such communication;”
- c. “to a person employed or authorized, or whose facilities are used, to forward such communication to its destination;” or
- d. “which were inadvertently obtained by the service provider and which appear to pertain to the commission of a crime, if such divulgence is made to a law enforcement agency.”

18 U.S.C. § 2511(3)(b).

275. Section 2511(2)(a)(i) provides:

It shall not be unlawful under this chapter for an operator of a switchboard, or an officer, employee, or agent of a provider of wire or electronic communication service, whose facilities are used in the transmission of a wire or electronic communication, to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service, except that a provider of wire communication service to the public shall not utilize service observing or random monitoring except for mechanical or service quality control checks.

276. Defendant’s divulgence of the contents of Plaintiff’s and Class Members’ communications on Defendant’s website to Facebook was not authorized by 18 U.S.C. § 2511(2)(a)(i) in that it was neither: (1) a necessary incident to the rendition of Defendant’s service; nor (2) necessary to the protection of the rights or property of Defendant.

277. Section 2517 of the ECPA relates to investigations by government officials and has no relevance here.

278. Defendant’s divulgence of the contents of user communications on Defendant’s Website through the Pixel was not done “with the lawful consent of the originator or any addressee or intend recipient of such communication[s].” As alleged above: (a) Plaintiff and Class Members did not authorize Defendant to divulge the contents of their communications; and (b) Defendant did not procure the “lawful consent” from the websites or apps with which Plaintiff and Class

Members were exchanging information.

279. Moreover, Defendant divulged the contents of Plaintiff's and Class Members' communications through the Pixel to individuals who are not "person[s] employed or whose facilities are used to forward such communication to its destination."

280. The contents of Plaintiff's and Class Members' communications did not appear to pertain to the commission of a crime and Defendant did not divulge the contents of their communications to a law enforcement agency.

281. As a result of the above actions and pursuant to 18 U.S.C. § 2520, the Court may assess statutory damages; preliminary and other equitable or declaratory relief as may be appropriate; punitive damages in an amount to be determined by a jury; and a reasonable attorney's fee and other litigation costs reasonably incurred.

COUNT IX

VIOLATION OF TITLE II OF THE ELECTRONIC COMMUNICATIONS PRIVACY ACT 18 U.S.C. § 2702, *et seq.* (STORED COMMUNICATIONS ACT) (On Behalf of Plaintiff & the Class)

282. Plaintiff repeats and re-alleges each and every allegation contained in the Complaint as if fully set forth herein.

283. The ECPA further provides that "a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service." 18 U.S.C. § 2702(a)(1).

284. **Electronic Communication Service.** ECPA defines "electronic communications service" as "any service which provides to users thereof the ability to send or receive wire or electronic communications." 18 U.S.C. § 2510(15).

285. Defendant intentionally procures and embeds various Plaintiff's PII and PHI through the Pixel used on Defendant's Website, which qualifies as an Electronic Communication Service.

286. **Electronic Storage.** ECPA defines "electronic storage" as "any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof" and "any storage of such communication by an electronic communication service for purposes of backup protection of such communication." 18 U.S.C. § 2510(17).

287. Defendant stores the content of Plaintiff's and Class Members' communications on Defendant's Website and files associated with it.

288. When Plaintiff or Class Members make a Website communication, the content of that communication is immediately placed into storage.

289. Defendant knowingly divulges the contents of Plaintiff's and Class Members' communications through the Pixel.

290. **Exceptions Do Not Apply.** Section 2702(b) of the Stored Communication Act provides that an electronic communication service provider "may divulge the contents of a communication—"

- a. "to an addressee or intended recipient of such communication or an agent of such addressee or intended recipient."
- b. "as otherwise authorized in Section 2517, 2511(2)(a), or 2703 of this title;"
- c. "with the lawful consent of the originator or an addressee or intended recipient of such communication, or the subscriber in the case of remote computing service;"
- d. "to a person employed or authorized or whose facilities are used to forward such communication to its destination;"

- e. “as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service;”
- f. “to the National Center for Missing and Exploited Children, in connection with a reported submission thereto under section 2258A.”
- g. “to a law enforcement agency, if the contents (i) were inadvertently obtained by the service provider; and (ii) appear to pertain to the commission of a crime;”
- h. “to a governmental entity, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of communications relating to the emergency”; or
- i. “to a foreign government pursuant to an order from a foreign government that is subject to an executive agreement that the Attorney General has determined and certified to Congress satisfies Section 2523.”

291. Defendant did not divulge the contents of Plaintiff’s and Class Members’ communications to “addressees,” “intended recipients,” or “agents” of any such addressees or intended recipients of Plaintiff and Class Members.

292. Section 2517 and 2703 of the ECPA relate to investigations by government officials and have no relevance here.

293. Section 2511(2)(a)(i) provides:

It shall not be unlawful under this chapter for an operator of a switchboard, or an officer, employee, or agent of a provider of wire or electronic communication service, whose facilities are used in the transmission of a wire or electronic communication, to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service, except that a provider of wire communication service to the public shall not utilize service observing or random monitoring except for mechanical or service quality control checks.

294. Defendant’s divulgence of the contents of Plaintiff’s and Class Members’ communications on Defendant’s Website to Facebook was not authorized by 18 U.S.C. §

2511(2)(a)(i) in that it was neither: (1) a necessary incident to the rendition of the Defendant's services; nor (2) necessary to the protection of the rights or property of Defendant.

295. Defendant's divulgence of the contents of user communications on Defendant's Website was not done "with the lawful consent of the originator or any addresses or intend recipient of such communication[s]." As alleged above: (a) Plaintiff and Class Members did not authorize Defendant to divulge the contents of their communications; and (b) Defendant did not procure the "lawful consent" from the websites or apps with which Plaintiff and Class Members were exchanging information.

296. Moreover, Defendant divulged the contents of Plaintiff and Class Members' communications through the Pixel to individuals who are not "person[s] employed or whose facilities are used to forward such communication to its destination."

297. The contents of Plaintiff's and Class Members' communications did not appear to pertain to the commission of a crime and Defendant did not divulge the contents of their communications to a law enforcement agency.

298. As a result of the above actions and pursuant to 18 U.S.C. § 2520, the Court may assess statutory damages; preliminary and other equitable or declaratory relief as may be appropriate; punitive damages in an amount to be determined by a jury; and a reasonable attorney's fee and other litigation costs reasonably incurred.

COUNT X

VIOLATION OF THE COMPUTER FRAUD AND ABUSE ACT (CFAA)

18 U.S.C. § 1030, *et seq.*

(On Behalf of Plaintiff & the Class)

299. Plaintiff repeats and re-alleges each and every allegation contained in the Complaint as if fully set forth herein.

300. Plaintiff's and Class Members' mobile devices are, and at all relevant times have been, used for interstate communication and commerce, and are therefore "protected computers" under 18 U.S.C. § 1030(e)(2)(B).

301. Defendant exceeded, and continues to exceed, authorized access to the Plaintiff's and Class Members' protected computers and obtained information thereby, in violation of 18 U.S.C. § 1030(a)(2), (a)(2)(C).

302. Defendant's conduct caused "loss to 1 or more persons during any 1-year period . . . aggregating at least \$5,000 in value" under 18 U.S.C. § 1030(c)(4)(A)(i)(I), *inter alia*, because of the secret transmission of Plaintiff's and Class Members' private and personally identifiable data and content – including the Website visitor's electronic communications with the Website, including their mouse movements, clicks, keystrokes (such as text being entered into an information field or text box), URLs of web pages visited, and/or other electronic communications in real-time ("Website Communications") which were never intended for public consumption.

303. Defendant's conduct also constitutes "a threat to public health or safety" under 18 U.S.C. § 1030(c)(4)(A)(i)(IV), due to the private and personally identifiable data and content of Plaintiff's and Class Members' Website Communications being made available to Defendant, Facebook, and/or other third parties without adequate legal privacy protections.

304. Accordingly, Plaintiff and Class Members are entitled to "maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief." 18 U.S.C. § 1030(g).

PRAYER FOR RELIEF

WHEREFORE, Plaintiff Carol Kane respectfully prays for judgment as follows:

- A. For an Order certifying this action as a Class action and appointing Plaintiff as Class Representative and Plaintiff's counsel as Class Counsel;
- B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class Members' Private Information, and from refusing to issue prompt, complete and accurate disclosures to Plaintiff and Class Members;
- C. For equitable relief compelling Defendant to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to disclose with specificity the type of PII and PHI disclosed to third parties;
- D. For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;
- E. For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;
- F. For an award of punitive damages, as allowable by law;
- G. For an award of attorneys' fees and costs, and any other expense, including expert witness fees;
- H. Pre- and post-judgment interest on any amounts awarded; and
- I. Such other and further relief as this court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff Carol Kane hereby demands that this matter be tried before a jury.

Date: January 11, 2023

Respectfully submitted,

WEITZ & LUXENBERG, PC

/s/ James J. Bilsborrow

James J. Bilsborrow
700 Broadway
New York, NY 10003
(212) 558-5500

*Counsel for Plaintiff and
the Nationwide Class*